ловии, что весь незаконный контент удален. Если в будущем будет обнаружен тот же самый контент, за который сайт был заблокирован, то доступ к сайту будет закрыт навсегда.

Весь этот комплекс обеспечит эффективную работу по устранению сайтов с пиратским контентом и принесет хорошую прибыль государству и авторам материалов.

РАЗРАБОТКА СИСТЕМЫ КОНСУЛЬТИРОВАНИЯ ДЛЯ ОПТИМИЗАЦИИ РАБОТЫ ПЕРСОНАЛА С УЧЕТОМ ВОЗМОЖНЫХ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Н. В. Аксенова, В. И. Белов, С. О. Суханинский
(Курган, КГУ, naaks@yandex.ru)
Научный руководитель: канд. техн. наук, доцент *А. П. Головко*

Человеческий фактор играет существенную роль в системе обеспечения безопасности информации, и человек, являясь пользователем информационной системы, был и остается одним из самых уязвимых ее мест. Люди, работающие с информацией, могут рассматриваться как звено в цепочке механизма, который обеспечивает работоспособность и безопасность всей системы.

Существуют системы экспресс-оценки лояльности сотрудника Trustee и экспресс-оценки благонадежности кандидата на работу Integritest. Обе системы разработаны фирмой MIDOT и являются платными. Это системы онлайн-тестирования. Результат не требует интерпретации, влияние человеческого фактора при формировании результата исключено.

Лояльность сотрудников и кандидатов на должность также оценивают с помощью полиграфа. Детектор лжи и последующие этапы его развития – MindReader, Sprint – способны с очень высокой долей вероятности получить информацию из прошлого и о прошлом. Полиграф не способен анализировать суждения и мнения и, соответственно, делать прогноз. На это способен специалист, исходя из личного жизненного и профессионального опыта. В основе

профессионализма полиграфолога также лежат все те же элементарные человеческие честность и порядочность. Хороший специалист требует высокой оплаты. Услуги низкоквалифицированного специалиста могут привести к нежелательным последствиям.

В рамках создания политики информационной безопасности рассматриваются такие понятия, как «риски информационной безопасности» и «модель нарушителя».

Риск информационной безопасности (далее ИБ) представляет собой возможность нарушения ИБ с негативными последствиями.

Основными рисками ИБ являются:

– риск утечки конфиденциальной информации;

– риск потери или недоступности важных данных;

– риск использования неполной или искаженной информации;

– риск неправомочной скрытой эксплуатации информационно-вычислительных ресурсов;

– риск распространения информации, угрожающей репутации организации.

В соответствии с рисками и другими аспектами политики информационной безопасности составляют модель нарушителя информационной безопасности.

Модель нарушителя – абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа; предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

Модель нарушителя должна ответить на следующие вопросы:

1. Какие угрозы могут быть реализованы.
2. Кем могут быть реализованы эти угрозы.
3. С какой вероятностью могут быть реализованы эти угрозы.
4. Каков потенциальный ущерб от этих угроз.
5. Каким образом могут быть реализованы эти угрозы.
6. Почему эти угрозы могут быть реализованы.
7. На что могут быть направлены эти угрозы.
8. Как можно отразить эти угрозы.

По данным портала incidents.su за 2011 г. было зарегистрировано как минимум 850 инцидентов информационной безопасности,

из которых наиболее крупную группу составили утечки (451 случай, или 54 % от общего количества), когда DDoS-атаки и взломы составили 238 и 92, или 28 % и 11 % соответственно) [1]. Лидирующими являются утечки вида «несанкционированные действия», что свидетельствует о необходимости усиления внутреннего контроля над сотрудниками, работающими с информацией.

По данным портала infowatch.ru количество зарегистрированных преднамеренных и непреднамеренных утечек информации в 2011 г. было приблизительно одинаковым. В 2012 г. это соотношение изменилось в сторону увеличения количества преднамеренных утечек. Однако доля непреднамеренных утечек по-прежнему остается довольно большой.

Причины непреднамеренных утечек информации чаще всего связаны с деловыми, личностными и профессиональными качествами сотрудника.

Одно из наиболее важных мероприятий в работе с персоналом предприятия – процесс подбора возможных кандидатов для назначения на должности, связанные с конфиденциальной информацией. При подборе кандидатов специалистом кадрового отдела проводится оценка соответствия каждого из них следующим основным требованиям:

– уровню подготовки и квалификации, наличию необходимого опыта работы кандидата на должность;

– деловым и личностным качествам соискателя;

– степени ответственности за принимаемые решения (в зависимости от занимаемой должности) претендента.

К кандидатам на ту или иную должность предъявляются профессиональные требования в соответствии с должностными инструкциями, но также важно учитывать их деловые и личностные качества (см. таблицу).

Часто при приеме на работу в качестве одного из испытаний кандидата на должность используют психологическое тестирование с помощью различных методик, которое позволяет выявить наличие необходимых качеств, но не может быть причиной отказа при приеме на работу.

Деловые, личностные и профессиональные качества

Деловые качества	Личностные качества	Профессиональные качества
Исполнительность	Честность	Знание нормативных актов, регулирующих практическую деятельность
Ответственность	Принципиальность, эмоциональная устойчивость (самообладание)	Использование новых информационных и инновационных технологий
Дисциплинированность	Добросовестность	Знание проектной документации в своей деятельности
Инициативность	И т. д.	И т. д.
Способность выделить главное в работе, сконцентрироваться на решении наиболее важных вопросов		
Умеренная склонность к возможным рискам		
Наличие широкого кругозора, постоянное стремление к повышению уровня теоретических знаний и практических навыков		
Правильная оценка собственных способностей и возможностей		
И т. д.		

В таблице перечислены не все деловые, личностные и профессиональные качества. В каждом конкретном случае этот список рассматривается отдельно.

Причины преднамеренных нарушений информационной безопасности могут быть различными: подкуп сотрудника, возможность его шантажа, социальные и личностные проблемы сотрудника, желание сотрудника самовыразиться и т. д.

Эти причины выделены в блок, названный «Индикаторы неблагонадежности».

1. Безответственность, попустительство, недальновидность, халатность.

2. Демонстративность поведения, эксклюзив, тщеславие.

3. Зависть как черта характера. Интриганство.

4. Легкая внушаемость, доверчивость, подчиняемость.

5. Лживость как черта характера. Жуликоватость.

6. Негативные черты характера, такие как алчность, продажность.

7. Негативные эмоциональные черты характера: обидчивость, подлость, мстительность.

8. Неустойчивость к стрессам.

9. Резкие изменения настроения в течение дня.

10. Скрытность, усиленный самоконтроль.

11. Зависимость от чего-либо или от кого-либо.

12. Провокационные разговоры и действия.

13. Совершение нелогичных поступков.

14. Боязнь шантажа, наличие уязвимых мест.

15. Внезапное изменение материального положения. Жизнь не по доходам.

16. Желание сохранить должность, когда очевидно, что человек ее перерос.

17. Интерес к информации, представляющей коммерческую тайну.

18. Интерес к сложившимся межличностным отношениям.

19. Компрометирующий круг общения.

20. Крупные покупки за последние два-три месяца.

21. Крупный долг.

22. Наличие судимости.

23. Одиночество, отсутствие семьи, отсутствие иждивенцев.

24. Плохие жилищные условия и интенсивное желание их улучшить.

25. Принадлежность к малым неформальным группам, сектам.

26. Пристрастие к алкоголю, наркотикам.

27. Резкое изменение социального уровня.

28. Озабоченность вопросами секса. Разлад в семье.

29. Серьезное заболевание человека или его близких.

30. Страсть, стремление обладать чем-либо.

Индикаторы в большинстве своем тоже могут быть выявлены с помощью методик психологического тестирования, конкретных или общих. Некоторые индикаторы требуют иного подхода для своего определения.

По совету эксперта из множества существующих методик была выбрана методика многофакторного исследования личности Кэттела как наиболее универсальная, многомерная, оценивающая свойства личности, широкую сферу индивидуально-личностных отношений, личностную структуру человека и личностные проблемы, как более простая для работы неспециалиста-психолога и оптимальная по времени.

С помощью методических указаний к опроснику, разработанных интерпретаций множественных и парных сочетаний факторов опросника и указаний эксперта были выявлены факторы и сочетания факторов, определяющих то или иное качество.

Впоследствии были установлены соответствия между полученными после прохождения теста результатами (стенами) по каждому интересующему фактору и искомыми качествами.

Были определены три градации соответствия:

– отсутствует;

– слабое;

– сильное.

Аналогично исследованию деловых и личностных качеств было проведено исследование индикаторов неблагонадежности.

Также было выделено три степени соответствия:

– отсутствует;

– слабое;

– сильное.

Для проверки составленных методик определения характеристики и индикаторов в сочетаниях факторов применялась операция Т-нормы.

Проверка проводилась на двух выборках.

В первой выборке были использованы результаты тестирования студентов экономического факультета в возрасте 18 лет. В ходе исследования было выявлено, что эти данные не подтверждают выдвинутое предположение по оценке деловых и личностных качеств в связи с особенностью тестируемых (неработающие студенты до 20 лет). Во второй выборке были результаты 12 сотрудников не старше 25 лет с опытом работы не менее 3 лет. Сильный уровень

выраженности по деловым и личностным качествам выявлен в среднем у 3 человек из 12, слабый уровень выраженности – у 5 из 12.

Результаты обработки были признаны удовлетворительными.

После анализа полученных результатов был сделан вывод о возможности применения данного подхода к выявлению необходимых деловых и личностных качеств, а также индикаторов неблагонадежности.

В дальнейшем планируется, применяя функцию принадлежности в соответствии с указаниями эксперта, установить численное соответствие между качествами, индикаторами и списком выбранных должностей.

РАЗВИТИЕ КОМПЕТЕНЦИЙ БУДУЩИХ МЕНЕДЖЕРОВ В ОБЛАСТИ КАДРОВОЙ БЕЗОПАСНОСТИ В ВУЗЕ КАК ПЕДАГОГИЧЕСКАЯ ПРОБЛЕМА

А. А. Томилов
(Трехгорный, ЮУрГУ (национальный исследовательский университет), Tomilov62@ya.ru)

На сегодняшний день специалисты, отвечающие за безопасность предприятий, организаций и учреждений, признают, что кадровая безопасность – это непременная и основная составная часть любой системы, которую организация формирует для своей защиты.

Обычно при рассмотрении вопросов, связанных с кадровой безопасностью, часто подразумевают безопасность предприятия, организации, учреждения. Прежде всего хотелось бы сказать, что это – два абсолютно разных понятия, так как кадровая безопасность является одной из составляющих безопасности в целом, наряду с другими элементами, такими как финансовая, силовая, информационная, технико-технологическая, правовая, промышленная, экологическая безопасности. Невооруженным взглядом видно, что кадровая безопасность занимает доминирующее положение по отношению к другим элементам системы безопасности компа-